CLAIMS

What is claimed is:

1. A method of initializing a security module, the method comprising the acts of:

determining if the security module is a controlling security module or a subordinate security module;

generating at least one key if the security module is the controlling security module; and

receiving at least one key from another security module if the security module is the subordinate security module.

2. The method, as set forth in claim 1, comprising the act of initializing the security modules in a system so that the security module has at least one common key with another security module.

3. The method, as set forth in claim 1, wherein the security module comprises a trusted platform module (TPM).

4. The method, as set forth in claim 1, comprising the act of measuring a system once the at least one key is generated.

5. The method, as set forth in claim 4, wherein the controlling security module measures the system.

6. The method, as set forth in claim 4, comprising the act of copying the measurement of the system into the subordinate security module.

7. The method, as set forth in claim 1, wherein the at least one key comprises an endorsement key.

8. The method, as set forth in claim 1, wherein the at least one key comprises a private key and a public key.

9. The method, as set forth in claim 1, comprising the act of accessing a lock bit to determine if the security module is the controlling security module or the subordinate security module.

10. The method, as set forth in claim 9, wherein the lock bit is a setting within memory of the system.

11. The method, as set forth in claim 10, comprising accessing the lock bit via a bus coupled to the security module and the memory or via a bus and a input/output controller coupled between the security module and the memory.

12. The method, as set forth in claim 10, comprising the act of determining if the security module in the system is initialized.

13. A security module, comprising:

a detector that is adapted to determine if the security module is a controlling security module or a subordinate security module;

a key generator that generates a key for the security module if the security module is the controlling security module; and

a key receiver that receives the key from another security module if the security module is the subordinate security module.

14. The security module set forth in claim 13, wherein the security module comprises a trusted platform module ("TPM").

15. The security module set forth in claim 14, wherein the security module is adapted to determine if the security module has undergone TPM initialization.

16. The security module, as set forth in claim 14, wherein the key comprises an endorsement key.

17. The security module, as set forth in claim 14, wherein the key comprises a private key.

18. The security module set forth in claim 13, wherein the security module is adapted to measure a computer system if the security module is the controlling security module.

19. The security module set forth in claim 13, wherein the security module is adapted to access a lock bit to determine if the security module is the controlling security module or the subordinate security module.

20. The security module set forth in claim 19, comprising accessing the lock bit via a bus coupled to the security module and the memory or via a bus and a input/output controller coupled between the security module and the memory.

21. A security module, comprising:

means for determining if another security module is a controlling security module or a subordinate security module;

means for generating at least one key for the other security module if the other security modules is the controlling security module; and

means for receiving at least one key from the other security module if the other security module is the subordinate security module.

22. The security module as set forth in claim 21, wherein the controlling security module is adapted to measure a computer system.

23. A computer system, comprising:

a processor;

a hard disk operatively coupled to the processor and configured to store data for the processor;

a memory operatively coupled to the processor and configured to store data retrieved from the hard disk for use by the processor;

a video controller operatively coupled to the processor and configured to produce a display signal;

a first security module and a second security module, each operatively coupled to the processor and the memory, the first and second security modules being configured to:

determine whether the first security module or the second security module is a controlling security module or a subordinate security module;

generate at least one key for the first security module or the second security module depending on whether the first security module or the second security module is the controlling security module; and

receiving at least one key from the first security module or the second security module depending on whether the first security module or the second security module is the subordinate security module.

24. The computer system set forth in claim 23, wherein the first security module and the second security module each comprise a trusted platform module ("TPM").

25. The computer system set forth in claim 24, wherein the at least one key comprises an endorsement key.

26. The computer system set forth in claim 24, wherein the at least one key comprises a private key and a public key.

27. The computer system set forth in claim 23, wherein the first security module and the second security module are each adapted to determine if that security module has undergone TPM initialization.

28. The computer system set forth in claim 23, wherein the controlling security module is adapted to measure a computer system.

29. The computer system set forth in claim 23, wherein the first security module and the second security module are adapted to access a lock bit to determine if that security module is the controlling security module or the subordinate security module.

30. The computer system set forth in claim 23, wherein the memory and the first security module are connected together on a bus and communicate through a bridge with the processor.

31. A method of initializing a plurality of security modules in a computer system, the method comprising the act of:

initializing each of the plurality of security modules so that each of the plurality of security modules has at least one common key.

32. The method, as set forth in claim 31, wherein each of the plurality of security modules comprises a trusted platform module ("TPM").

33. The method, as set forth in claim 31, comprising accessing a lock bit in a memory by each of the plurality of security modules if the security module has not been initialized.

34. The method, as set forth in claim 33, wherein at least one of the plurality of security modules is coupled to a bus that connects to the memory.

35. The method, as set forth in claim 31, comprising booting the computer system once the plurality of security modules is initialized.

36. A networked computer system comprising:

a plurality of computer systems;

a network coupled to each of the plurality of computer systems;

at least one of the plurality of computer systems comprising:

a first security module and a second security module being configured to:

determine whether the first security module or the second security module is a controlling security module or a subordinate security module;

generate at least one key for the first security module or the second security module depending on whether the first security module or the second security module is the controlling security module; and

receiving at least one key from the first security module or the second security module depending on whether the first security module or the second security module is the subordinate security module.

37. The system, as set forth in claim 36, wherein the first and the second security modules comprise a trusted platform module ("TPM").